



National Aeronautics and
Space Administration
Washington, DC 20546

Procurement Notice

PN 04-25
June 19, 2007

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY (IT) RESOURCES

BACKGROUND: NASA's contract requirements for IT Security are defined in the clause at NFS 1852.204-76, Security Requirements for Unclassified Information Technology Resources. In order to comply with the updated requirements of NASA Procedural Requirements (NPR) 2810, "Security of Information Technology," and to ensure consistency with the Government-wide requirements of the Federal Information Security Management Act of 2002 (FISMA), this Procurement Notice (PN) revises the NASA FAR Supplement (NFS) to:

- Expand the requirements for IT Security Plans to include a risk assessment and a Federal Information Processing Standards (FIPS) 199 assessment;
- Add a requirement for a Contingency Plan; and
- Change the physical security requirement from a National Agency Check to a National Agency Check with Inquiries.

ACQUISITIONS AFFECTED BY CHANGES:

New Solicitations and Contracts: The revised clause at 1852.204-76 is applicable to all new NASA solicitations and contracts that require contractors to: (1) have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or (2) use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on NASA's or a contractor's information system.

Existing Contracts: Within 30 days after the date of this PN, contracting officers must identify existing contracts that meet the requirements of (1) or (2) above and whose period of performance extends beyond December 31, 2007. Contracting officers shall refer such contracts to the Center Chief Information Officer (CIO) for a determination as to which of those contracts must be modified to include the revised clause at 1852.204-76. All contract modifications should be completed within 90 days after the CIO's determination. Contracting officers shall document the contract file regarding consultation with the CIO on this issue, including the CIO's determination as to whether or not a contract must be modified.

ACTION REQUIRED BY CONTRACTING OFFICERS: Use the revised clause in new solicitations and contracts as prescribed in 1804.470-4, and modify existing contracts as directed by the Center CIO.

CLAUSE CHANGES: 1852.204-76, Security Requirements for Unclassified Information Technology Resources, is revised.

PARTS AFFECTED: Parts 1804 and 1852.

REPLACEMENT PAGES: You may use the enclosed pages to replace 4:1, 4:2, 4:3, 4:4, 52:5, 52:6, 52:7, 52:8, 52:9, 52:10, 52:10.1 (added) of the NFS.

TYPE OF RULE AND PUBLICATION DATE: The PN was published as a final rule in the Federal Register (72 FR 26560 - 26563) on May 10, 2007.

HEADQUARTERS CONTACT: Ken Stepka, Office of Procurement, Analysis Division, (202) 358-0492, email: ken.stepka@nasa.gov.

//s//

James A. Balinskas
Director, Contract Management Division

Enclosures

DISTRIBUTION LIST:
PN List

PART 1804
ADMINISTRATIVE MATTERS

TABLE OF CONTENTS

SUBPART	1804.1	CONTRACT EXECUTION
1804.103		Contract clause.
1804.170		Contract effective date.
SUBPART	1804.2	CONTRACT DISTRIBUTION
1804.202		Agency distribution requirements.
1804.203		Taxpayer identification information.
SUBPART	1804.4	SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY
1804.402		General.
1804.404-70		Contract clause.
1804.470		Security requirements for unclassified information technology (IT) resources
1804.470-1		Scope.
1804.470-2		Policy.
1804.470-3		IT Security Requirements.
1804.470-4		Contract clauses.
SUBPART	1804.5	ELECTRONIC COMMERCE IN CONTRACTING
1804.570		NASA Acquisition Internet Service (NAIS).
1804.570-1		General.
1804.570-2		Electronic Posting System.
SUBPART	1804.6	CONTRACT REPORTING
1804.601		Record requirements.
1804.604		Responsibilities.
1804.671		Committee on Academic Science and Engineering (C.A.S.E.) Report.
SUBPART	1804.8	GOVERNMENT CONTRACT FILES
1804.802-70		Handling of classified material.
1804.803		Contents of contract files.
1804.803-70		Checklist.
1804.804		Closeout of contract files.
1804.804-2		Closeout of the contracting office files if another office administers the contract.
1804.804-5		Procedures for closing out contract files.
1804.805		Storage, handling, and disposal of contract files.
1804.805-70		Review, separation, and retirement of contract files.

SUBPART	1804.9	TAXPAYER IDENTIFICATION NUMBER
1804.904		Reporting payment information to the IRS.
SUBPART	1804.70	TRANSFER OF CONTRACTING OFFICE RESPONSIBILITY
1804.7000		Scope of subpart.
1804.7001		Definition.
1804.7002		Approval of Transfer Requests.
1804.7003		Responsibilities of the contracting officer of the transferring installation.
1804.7003-1		Coordinations.
1804.7003-2		File inventory.
1804.7003-3		Notifications.
1804.7003-4		Transfer.
1804.7003-5		Retention documentation.
1804.7004		Responsibilities of the contracting officer of the receiving installation.
1804.7004-1		Pre-transfer file review.
1804.7004-2		Post-transfer actions.
SUBPART	1804.71	UNIFORM ACQUISITION INSTRUMENT IDENTIFICATION
1804.7100		Scope of subpart.
1804.7101		Policy.
1804.7102		Numbering scheme for solicitations.
1804.7103		Numbering scheme for contracts.
1804.7104		Modifications of contracts or agreements.
SUBPART	1804.72	REVIEW AND APPROVAL OF CONTRACTUAL INSTRUMENTS
1804.7200		Contract review by Headquarters.
SUBPART	1804.73	PROCUREMENT REQUESTS
1804.7301		General.

PART 1804 ADMINISTRATIVE MATTERS

Subpart 1804.1--Contract Execution

1804.103 Contract clause.

The contracting officer shall include the clause at FAR 52.204-1, Approval of Contract, in solicitations, contracts, and supplemental agreements that require higher level approval. For actions requiring Headquarters approval, insert "NASA Assistant Administrator for Procurement" in the clause's blank space.

1804.170 Contract effective date.

(a) "**Contract effective date**" means the date agreed upon by the parties for beginning the period of performance under the contract. In no case shall the effective date precede the date on which the contracting officer or designated higher approval authority signs the document.

(b) Costs incurred before the contract effective date are unallowable unless they qualify as precontract costs (see FAR 31.205-32) and the clause prescribed at 1831.205-70 is used.

Subpart 1804.2--Contract Distribution**1804.202 Agency distribution requirements.**

In addition to the requirements in FAR 4.201, the contracting officer shall distribute one copy of each R&D contract, including the Statement of Work, to the NASA Center for AeroSpace Information (CASI), Attention: Acquisitions Collections Development Specialist, 7115 Standard Drive, Hanover, MD 21076-1320.

1804.203 Taxpayer identification information.

Instead of using the last page of the contract to provide the information listed in FAR 4.203, NASA installations may allow contracting officers to use a different distribution method, such as annotating the cover page of the payment office copy of the contract.

Subpart 1804.4--Safeguarding Classified Information Within Industry**1804.402 General.**

(b) NASA security policies and procedures are prescribed in NPD 1600.2, NASA Security Policy; NPR 1620.2, Physical Security Vulnerability Risk Assessments; NPR 2810.1 Security of Information Technology; and NPD 2810.1, NASA Information Security Policy.

1804.404-70 Contract clause.

The contracting officer shall insert the clause at 1852.204-75, Security Classification Requirements, in solicitations and contracts if work to be performed will require security clearances. This clause may be modified to add instructions for obtaining security clearances and access to security areas that are applicable to the particular acquisition and installation.

1804.470 Security requirements for unclassified information technology (IT) resources.**1804.470-1 Scope.**

This section implements NASA's acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems. Federal policies include the Federal Information System Management Act (FISMA) of 2002, Homeland Security Presidential Directive (HSPD) 12, Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.), OMB Circular A-130, Management of Federal Information Resources, and the National Institute of Standards and Technology (NIST) security requirements and standards. These requirements safeguard IT services provided to NASA such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems.

1804.470-2 Policy.

NASA IT security policies and procedures for unclassified information and IT are prescribed in NASA Policy Directive (NPD) 2810, Security of Information Technology; NASA Procedural Requirements (NPR) 2810, Security of Information Technology; and interim policy updates in the form of NASA Information Technology Requirements (NITR). IT services must be performed in accordance with these policies and procedures.

1804.470-3 IT Security Requirements.

These IT security requirements cover all NASA contracts in which IT plays a role in the provisioning of services or products (e.g., research and development, engineering, manufacturing, IT outsourcing, human resources, and finance) that support NASA in meeting its institutional and mission objectives. These requirements are applicable where a contractor or subcontractor must obtain physical or electronic (i.e., authentication level 2 and above as defined in NIST Special Publication 800-63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure. These requirements are also applicable in cases where information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, is stored, generated, processed, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

1804.470-4 Contract clause.

(a) Insert the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources, in all solicitations and contracts when contract performance requires contractors to --

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, process, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(b) Paragraph (d) of the clause allows contracting officers to waive the requirements of paragraphs (b) and (c)(1) through (3) of the clause. Contracting officers must obtain the approval of the --

(1) Center IT Security Manager before granting any waivers to paragraph (b) of the clause; and

(2) The Center Chief of Security before granting any waivers to paragraphs (c)(1) through (3) of the clause.

(4) The NFS matrix may be reproduced by field installations for the purpose of supplementing it with installation-developed provisions and clauses.

1852.103 Identification of provisions and clauses.

(b) Provisions and clauses prescribed by a field installation to satisfy its needs shall be identified as stated in paragraphs (b)(i) and (ii) of this section. Articles, formats, and similar language shall be treated as provisions and clauses for purposes of this section 1852.103.

(i) A provision or clause shall be numbered using a prefix, a base, and a suffix. The prefix shall be an alphabetical abbreviation of the installation name (e.g., ARC, DFRC, GRC, GSFC, JSC, KSC, LARC, MSFC, SSC, or SSPO). The base shall be a numeric value beginning with "52.2," with the next two digits corresponding to the number of the FAR or NFS subject part to which the provision or clause relates. The suffix shall be a hyphen and sequential number assigned within each part. NASA installations shall use suffix numbers from -90 to -199. For example, the first Johnson Space Center (JSC) provision or clause relating to Part 36 of the FAR or NFS shall be JSC 52.236-90, the second JSC 52.236-91, and so forth. Provisions and clauses shall be dated in accordance with FAR 52.101(f).

(ii) Contracting officers shall identify provisions and clauses as in the following examples:

(A) ***1.2 BID ENVELOPES (GSFC 52.214-90) (AUGUST 1987)*** This example is applicable when identifying the title of provisions and clauses in solicitations and contracts using the uniform contract format (UCF). The first number ("1.2") designates the UCF section and the sequential clause within that section. "GSFC 52.214-90" specifies the clause number.

(B) ***GSFC 52.214-90--Bid Envelopes (AUGUST 1987)*** This example is applicable in all instances in which the provision or clause citation is not associated with the UCF number.

(c) Contracting officers shall not number provisions and clauses developed for individual acquisitions only. For example, "F.3 Delivery Procedures for Special Hardware" cites the third clause in Section F of a contract using the UCF, but has no clause number or date identified with it, indicating that the clause was developed for the particular contract it appears in.

1852.103-70 Identification of modified provisions and clauses.

When a FAR clause or provision is included in a solicitation or contract and the NFS prescribes a modification, the title line shall identify the modification as shown below. This format shall be used both for incorporation by reference and when using full text.

"52.232-28 Electronic Funds Transfer Payment Methods (APR 1989)--as modified by NASA FAR Supplement 1832.908(a)"

1852.104 Procedures for modifying and completing provisions and clauses.

NFS provisions and clauses shall not be modified unless authorized by the NFS. When authorized, contracting officers must comply with the procedures in FAR 52.104.

Subpart 1852.2--Text of Provisions and Clauses

1852.203-70 Display of Inspector General Hotline Posters.

As prescribed in 1803.7001, insert the following clause:

**DISPLAY OF INSPECTOR GENERAL HOTLINE POSTERS
(JUNE 2001)**

(a) The Contractor shall display prominently in common work areas within business segments performing work under this contract, Inspector General Hotline Posters available under paragraph (b) of this clause.

(b) Inspector General Hotline Posters may be obtained from NASA Office of Inspector General, Code W, Washington, DC, 20546-0001, (202) 358-1220.

(End of clause)

1852.204-75 Security Classification Requirements.

As prescribed in 1804.404-70, insert the following clause:

**SECURITY CLASSIFICATION REQUIREMENTS
(SEPTEMBER 1989)**

Performance under this contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of _____ [insert the applicable security clearance level]. See Federal Acquisition Regulation clause 52.204-2 in this contract and DD Form 254, Contract Security Classification Specification, Attachment ____ [Insert the attachment number of the DD Form 254].

(End of clause)

1852.204-76 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1804.470-4(a), insert the following clause:

**SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION
TECHNOLOGY RESOURCES
(MAY 2007)**

(a) The Contractor shall be responsible for information and information technology (IT) security when –

(1) The Contractor or its subcontractors must obtain physical or electronic (i.e., authentication level 2 and above as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure; or

(2) Information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems is stored, generated, processed, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

(b) IT Security Requirements.

(1) Within 30 days after contract award, a Contractor shall submit to the Contracting Officer for NASA approval an IT Security Plan, Risk Assessment, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Assessment. These plans and assessments, including annual updates shall be incorporated into the contract as compliance documents.

(i) The IT system security plan shall be prepared consistent, in form and content, with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, and any additions/augmentations described in NASA Procedural Requirements (NPR) 2810, Security of Information Technology. The security plan shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of Federal Information Processing Standards (FIPS) 200, Recommended Security Controls for Federal Information Systems. The plan shall be reviewed and updated in accordance with NIST SP 800-

26, Security Self-Assessment Guide for Information Technology Systems, and FIPS 200, on a yearly basis.

(ii) The risk assessment shall be prepared consistent, in form and content, with NIST SP 800-30, Risk Management Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The risk assessment shall be updated on a yearly basis.

(iii) The FIPS 199 assessment shall identify all information types as well as the “high water mark,” as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.

(2) The Contractor shall produce contingency plans consistent, in form and content, with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The Contractor shall perform yearly “Classroom Exercises.” “Functional Exercises,” shall be coordinated with the Center CIOs and be conducted once every three years, with the first conducted within the first two years of contract award. These exercises are defined and described in NIST SP 800-34.

(3) The Contractor shall ensure coordination of its incident response team with the NASA Incident Response Center (NASIRC) and the NASA Security Operations Center, ensuring that incidents are reported consistent with NIST SP 800-61, Computer Security Incident Reporting Guide, and the United States Computer Emergency Readiness Team’s (US-CERT) Concept of Operations for reporting security incidents. Specifically, any confirmed incident of a system containing NASA data or controlling NASA assets shall be reported to NASIRC within one hour that results in unauthorized access, loss or modification of NASA data, or denial of service affecting the availability of NASA data.

(4) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPR 2810 requirements. The Contractor may use web-based training available from NASA to meet this requirement.

(5) The Contractor shall provide NASA, including the NASA Office of Inspector General, access to the Contractor’s and subcontractors’ facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out IT security inspection, investigation, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA information or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime. To facilitate mandatory reviews, the Contractor shall ensure appropriate compartmentalization of NASA information, stored and/or processed, either by information systems in direct support of the contract or that are incidental to the contract.

(6) The Contractor shall ensure that system administrators who perform tasks that have a material impact on IT security and operations demonstrate knowledge appropriate to those tasks. Knowledge is demonstrated through the NASA System Administrator Security Certification Program. A system administrator is one who provides IT services (including network services, file storage, and/or web services) to someone other than themselves and takes or assumes the responsibility for the security and administrative controls of that service. Within 30 days after contract award, the Contractor shall provide to the Contracting Officer a list of all system administrator positions and personnel filling those positions, along with a schedule that ensures certification of all personnel within 90 days after contract award. Additionally, the Contractor should report all personnel changes which impact system administrator positions within 5 days of the personnel change and ensure these individuals obtain System Administrator certification within 90 days after the change.

(7) The Contractor shall ensure that NASA's Sensitive But Unclassified (SBU) information as defined in NPR 1600.1, NASA Security Program Procedural Requirements, which includes privacy information, is encrypted in storage and transmission.

(8) When the Contractor is located at a NASA Center or installation or is using NASA IP address space, the Contractor shall --

(i) Submit requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the Network Security Configuration Control Board (NSCCB);

(ii) Comply with the NASA CIO metrics including patch management, operating systems and application configuration guidelines, vulnerability scanning, incident reporting, system administrator certification, and security training; and

(iii) Utilize the NASA Public Key Infrastructure (PKI) for all encrypted communication or non-repudiation requirements within NASA when secure email capability is required.

(c) Physical and Logical Access Requirements.

(1) Contractor personnel requiring access to IT systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPR 2810 and Chapter 4, NPR 1600.1, NASA Security Program Procedural Requirements. NASA shall provide screening, appropriate to the highest risk level, of the IT systems and information accessed, using, as a minimum, National Agency Check with Inquiries (NACI). The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of NASA, interim access may be granted pending completion of the required investigation and final access determination. For Contractors who will reside on a NASA Center or installation, the security screening required for all required access (e.g., installation, facility, IT, information, etc.) is consolidated to ensure only one investigation is conducted based on the highest risk level. Contractors not residing on a NASA installation will be screened based on their IT access risk level determination only. See NPR 1600.1, Chapter 4.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT-1 has the highest level of risk).

(i) IT-1 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT-2 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of "level 1" information whose cost to replace exceeds one million dollars.

(iii) IT-3 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the Contractor for NASA whose function or information has substantial cost to replace, even if these systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as established in Chapter 4, NPR 1600.1.

(4) The Contractor may conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate to the Contracting Officer that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures for the risk level assigned for the IT position.

(5) Subject to approval of the Contracting Officer, the Contractor may forgo screening of Contractor personnel for those individuals who have proof of a --

(i) Current or recent national security clearances (within last three years);

(ii) Screening conducted by NASA within the last three years that meets or exceeds the screening requirements of the IT position; or

(iii) Screening conducted by the Contractor, within the last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer and concurred on by the CCS.

(d) The Contracting Officer may waive the requirements of paragraphs (b) and (c)(1) through (c)(3) upon request of the Contractor. The Contractor shall provide all relevant information requested by the Contracting Officer to support the waiver request.

(e) The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

(f) At the completion of the contract, the contractor shall return all NASA information and IT resources provided to the contractor during the performance of the contract and certify that all NASA information has been purged from contractor-owned systems used in the performance of the contract.

(g) The Contractor shall insert this clause, including this paragraph (g), in all subcontracts

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, process, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(End of clause)

1852.208-81 Restrictions on Printing and Duplicating.

As prescribed in 1808.870, insert the following clause:

RESTRICTIONS ON PRINTING AND DUPLICATING (NOVEMBER 2004)

(a) The Contractor may duplicate or copy any documentation required by this contract in accordance with the provisions of the Government Printing and Binding Regulations, No. 26, S. Pub 101-9, U.S. Government Printing Office, Washington, DC, 20402, published by the Joint Committee on Printing, U.S. Congress.

(b) The Contractor shall not perform, or procure from any commercial source, any printing in connection with the performance of work under this contract. The term "printing" includes the processes of composition, platemaking, presswork, duplicating, silk screen processes, binding, microform, and the end items of such processes and equipment.

(c) The Contractor is authorized to duplicate or copy production units provided the requirement does not exceed 5,000 production units of any one page or 25,000 units in the aggregate of multiple pages. Such pages may not exceed a maximum image size of 10-3/4 by 14-1/4 inches. A "production unit" is one sheet, size 8-1/2 x 11 inches (215 x 280 mm), one side only, and one color ink.

(d) This clause does not preclude writing, editing, preparation of manuscript copy, or preparation of related illustrative material as a part of this contract, or administrative

duplicating/copying (for example, necessary forms and instructional materials used by the Contractor to respond to the terms of the contract).

(e) Costs associated with printing, duplicating, or copying in excess of the limits in paragraph (c) of this clause are unallowable without prior written approval of the Contracting Officer. If the Contractor has reason to believe that any activity required in fulfillment of the contract will necessitate any printing or substantial duplicating or copying, it immediately shall provide written notice to the Contracting Officer and request approval prior to proceeding with the activity. Requests will be processed by the Contracting Officer in accordance with the provisions of the Government Printing and Binding Regulations, NFS 1808.802, and NPR 1490.5, NASA Procedural Requirements for Printing, Duplicating, and Copying Management.

(f) The Contractor shall include in each subcontract which may involve a requirement for any printing, duplicating, and copying in excess of the limits specified in paragraph (c) of this clause, a provision substantially the same as this clause, including this paragraph (f).

(End of clause)

1852.209-70 Product Removal from Qualified Products List.

As prescribed in 1809.206-71, insert the following clause:

PRODUCT REMOVAL FROM QUALIFIED PRODUCTS LIST (DECEMBER 1988)

If, during the performance of this contract, the product being furnished is removed from the Qualified Products List for any reason, the Government may terminate the contract for Default pursuant to the default clause of the contract.

(End of clause)

1852.209-71 Limitation of Future Contracting.

As prescribed in 1809.507-2, the contracting officer may insert a clause substantially as follows in solicitations and contracts, in compliance with FAR 9.507-2:

LIMITATION OF FUTURE CONTRACTING (DECEMBER 1988)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict is [describe the conflict].

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing NASA contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). NASA shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

1852.209-72 Composition of the Contractor.

As prescribed in 1809.670, insert the following clause:

**COMPOSITION OF THE CONTRACTOR
(DECEMBER 1988)**

If the Contractor is comprised of more than one legal entity, each entity shall be jointly and severally liable under this contract.

(End of clause)

1852.211-70 Packaging, Handling, and Transportation

As prescribed in 1811.404-70, insert the following clause:

**PACKAGING, HANDLING, AND TRANSPORTATION
(SEPTEMBER 2005)**

(a) The Contractor shall comply with NASA Procedural Requirements (NPR) 6000.1, "Requirements for Packaging, Handling, and Transportation for Aeronautical and Space Systems, Equipment, and Associated Components", as may be supplemented by the statement of work or specifications of this contract, for all items designated as Class I, II, or III.

(b) The Contractor's packaging, handling, and transportation procedures may be used, in whole or in part, subject to the written approval of the Contracting Officer, provided (1) the Contractor's procedures are not in conflict with any requirements of this contract, and (2) the requirements of this contract shall take precedence in the event of any conflict with the Contractor's procedures.

(c) The Contractor must place the requirements of this clause in all subcontracts for items that will become components of deliverable Class I, II, or III items.

(End of clause)